The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
09/23/2021

SUBJECT:
Multiple Vulnerabilities in Nagios Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Nagios, the most severe of which could allow for remote code execution. Nagios is an open source monitoring system for computer systems. Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution. Depending on the privileges associated with the application, an attacker could view, change, or delete data. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Nagios XI versions prior to 5.8.5
- Nagios XI Switch Wizard versions prior to 2.5.7
- Nagios XI Docker Wizard versions prior to 1.1.3
- Nagios XI WatchGuard versions prior to 1.4.8

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Nagios, the most severe of which could allow for remote code execution. Details of the vulnerabilities are as follows:

- A path traversal vulnerability exists in Nagios XI below version 5.8.5 AutoDiscovery component and could lead to post-authenticated RCE under the security context of the user running Nagios. (CVE-2021-37343)
- Nagios XI Switch Wizard before version 2.5.7 is vulnerable to remote code execution through improper neutralization of special elements used in an OS Command (OS Command injection). (CVE-2021-37344)
- Nagios XI before version 5.8.5 is vulnerable to local privilege escalation because xi-sys.cfg is being imported from the var directory for some scripts with elevated permissions. (CVE-2021-37345)
- Nagios XI WatchGuard Wizard before version 1.4.8 is vulnerable to remote code execution through Improper neutralization of special elements used in an OS Command (OS Command injection). (CVE-2021-37346)
- Nagios XI before version 5.8.5 is vulnerable to local privilege escalation because getprofile.sh does not validate the directory name it receives as an argument. (CVE-2021-37347)
- Nagios XI before version 5.8.5 is vulnerable to local file inclusion through an improper limitation of a pathname in index.php. (CVE-2021-37348)
- Nagios XI before version 5.8.5 is vulnerable to local privilege escalation because cleaner.php does not sanitize input read from the database. (CVE-2021-37349)
- Nagios XI before version 5.8.5 is vulnerable to SQL injection vulnerability in Bulk Modifications Tool due to improper input sanitization. (CVE-2021-37350)
- Nagios XI before version 5.8.5 is vulnerable to insecure permissions and allows unauthenticated users to access guarded pages through a crafted HTTP request to the server. (CVE-2021-37351)
- An open redirect vulnerability exists in Nagios XI before version 5.8.5 that could lead to spoofing. To exploit the vulnerability, an attacker could send a link that has a specially-crafted URL and convince the user to click the link. (CVE-2021-37352)
- Nagios XI Docker Wizard before version 1.1.3 is vulnerable to SSRF due to improper sanitization in table_population.php. (CVE-2021-37353)

Successful exploitation of the most severe of these vulnerabilities could allow for remote code execution. Depending on the privileges associated with the application, an attacker could view, change, or delete data. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:
The following actions should be taken:
- Apply appropriate updates provided by Nagios to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Nagios:

https://www.nagios.com/products/security/

TheHackerNews:
https://thehackernews.com/2021/09/new-nagios-software-bugs-could-let.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37343
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37344
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37345
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37346
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37347
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37348
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37349
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37350
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37351
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37352
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37353

TLP: WHITE
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.